(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－358418
（P2002－358418A）
(43)公開日　平成14年12月13日(2002.12.13)

| (51)Int.Cl.' | 識別記号 | ＦＩ | テーマコード'(参考) |
|---|---|---|---|
| Ｇ０６Ｆ　17/60 | ２２４ | Ｇ０６Ｆ　17/60 | ２２４　３Ｅ０４４ |
| | ２３６ | | ２３６Ａ |
| | ５１２ | | ５１２ |
| Ｇ０７Ｆ　7/10 | | Ｇ０７Ｆ　7/10 | |

審査請求　有　請求項の数４　ＯＬ　（全 10 頁）

(21)出願番号　特願2001－164525(P2001－164525)

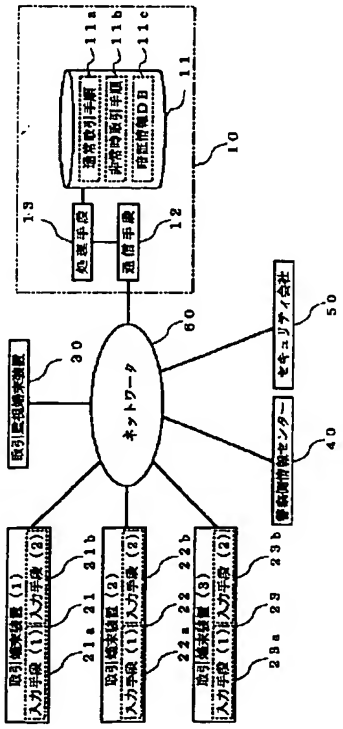
(22)出願日　平成13年５月31日(2001.5.31)

(71)出願人　300017337
元　英哲
東京都足立区関原２－６－４
(72)発明者　元　英哲
東京都足立区関原２丁目６番４号
(74)代理人　100110652
弁理士　塩野谷　英城

Ｆターム(参考)　3E044 AA20 DA06 DD02 DD03 DE01

(54)【発明の名称】　取引システム

(57)【要約】
【課題】　非常の事態に遭遇した際の自衛手段を、取引契約者に提供する。
【解決手段】　記憶手段１１に、一の取引契約者ＩＤに通常暗証情報と非常時暗証情報との双方を関連付けた組合せを取引契約者ＩＤ毎に複数記憶し、通常暗証情報に関連付けられた通常取引手順と、非常時暗証情報に関連付けられた非常時取引手順とを格納する。そして、取引端末装置２１から取引契約者ＩＤ及び暗証情報を通信手段１２を介して受信し、この取引契約者ＩＤと暗証情報との関連付けに一致する取引契約者ＩＤと通常暗証情報又は非常時暗証情報との関連付けを記憶手段１１から検索し、検索された関連付けをなす暗証情報が非常時暗証情報である場合、非常時取引手順を記憶手段１１から読み出して実行する。



1

【特許請求の範囲】

【請求項１】　情報の記憶手段と、取引端末装置との通信手段と、これら各手段の動作を制御する処理手段とを備え、

前記記憶手段は、一の取引契約者ＩＤに通常暗証情報と非常時暗証情報との双方を関連付けた組合せを前記取引契約者ＩＤ毎に複数記憶するとともに、前記通常暗証情報に関連付けられた通常取引手順と、前記非常時暗証情報に関連付けられた非常時取引手順とを記憶した取引システムであって、

前記処理手段は、

前記取引端末装置が認識した取引契約者ＩＤ及び暗証情報を前記通信手段を介して受信し、この取引契約者ＩＤと暗証情報との関連付けに一致する取引契約者ＩＤと通常暗証情報又は非常時暗証情報との関連付けを、前記記憶手段から検索するステップと、

検索された関連付けをなす暗証情報が前記非常時暗証情報である場合、前記非常時取引手順を前記記憶手段から読み出して実行するステップと、

を実行することを特徴とした取引システム。

【請求項２】　請求項１に記載の取引システムにおいて、

前記記憶手段は、一の取引契約者ＩＤについて、複数の異なる非常時暗証情報を格納すると共に、当該各非常時暗証情報について、各々異なる非常時取引手順を格納し、

前記処理手段は、前記検索された関連付けをなす暗証情報が前記非常時暗証情報である場合、当該非常時暗証情報に対応する非常時取引手順を前記記憶手段から選択的に読み出すことを特徴とした取引システム。

【請求項３】　請求項１に記載の取引システムにおいて、

前記記憶手段は、さらに、予め設定された非常時取引制限枠を前記取引契約者ＩＤ毎に関連付けて記憶すると共に、

前記処理手段は、前記非常時取引手順として、

前記受信した取引契約者ＩＤに対応する非常時取引制限枠を前記記憶手段から読み出すステップと、

当該読み出した非常時取引制限枠を通常の取引可能枠に見せかけて、前記取引端末装置へ前記通信手段を介して送信するステップと、

を実行することを特徴とした取引システム。

【請求項４】　請求項１に記載の取引システムにおいて、

前記処理手段は、前記非常時取引手順として、

前記受信した取引契約者ＩＤに基づいて非常時取引手順が要求されたことを示す報知情報を、前記通信手段を介し、当該非常時取引手順を要求した取引端末装置以外の外部装置に出力することを特徴とした取引システム。

【発明の詳細な説明】

2

【０００１】

【発明の属する技術分野】本発明は、取引システムに係り、特に、暗証情報を用いて取引契約者の認証を行う取引システムに関する。

【０００２】

【従来の技術】磁気カード等を用いた取引システムでは、暗証番号を用いた個人認証を行い、取引が正当な契約者との間で行われるように担保している。例えば、銀行では、キャッシュカードを使ってＡＴＭ（Automated Teller Machine）やＣＤ（Cash Dispenser）から現金を引き出す際に暗証番号の入力を必要とする。また、この暗証番号を用いた個人認証方法は、クレジットカードによるキャッシングの際にも用いられている。

【０００３】ここで、従前は、キャッシュカードやクレジットカードなどの磁気カードに取引契約者を特定するための口座番号と暗証番号を記憶させていた。しかし、不正にキャッシュカード等を入手した第三者が、磁気コードを読み取るカードリーダーなどにより暗証番号を読み出し、正当契約者になりすまして現金の不正な引き出しを行うなどの犯罪が横行したため、現在では磁気カードに個人認証のための暗証番号を記憶させずにホストコンピュータ側で暗証番号を管理するゼロ暗証方式が採用されている。

【０００４】また、磁気カードに代えて、ＩＣ（Integrated Circuit）カードをキャッシュカード等に採用し、第三者が不正にカードを取得しても容易に個人認証用の暗証情報が判明しないようにする手法にも注目が集まっている。

【０００５】例えば、特開２００１－６７３２２号公報には、ＩＣカードが複数の暗証番号あるいはそれに代わる取引契約者の指紋や虹彩などのデータを格納する構成が開示されている。

【０００６】

【発明が解決しようとする課題】しかしながら、上記従来例にあっては、キャッシュカード等を用いているのが取引契約者本人であるか否かを判別するにとどまっている。例えば、前述した特開２００１－６７３２２号公報に開示された複数の個人認証用情報を備えるシステムであっても、取引契約者本人か否かを判断するという技術的思想の域を脱するものではない。

【０００７】このため、第三者が銃刀による脅迫や暴行などを用いて取引契約者に現金の引き出しを強要し、取引契約者に自己の意思に反するかたちでキャッシュカード等を使用させた場合には、行為の主体の観点から見れば取引契約者本人が取引を行っているので、取引システムはその取引が通常ではない非常の取引であるとの区別はできない。したがって、取引システムは、取引契約者に対し上述したような非常の事態に対処し得る手段を何一つ提供できないという不都合があった。

【０００８】特に、銀行のサービス向上の一環として、

ＡＴＭなどを配したカードサービスコーナーを深夜も利用できる２４時間営業体制としたり、コンビニエンスストアなど、集団を形成していても違和感のない場所にＡＴＭを配置するようになってきている現状においては、上述したような犯罪のケースを取引契約者側の問題として単純に処理してしまうのは酷に過ぎる。

【０００９】また、インターネットなどの情報インフラストラクチャーが発達した今日では、ネットワークを用いて家庭にいながら銀行のサービスを受けることができる、いわゆるインターネットバンキングも浸透しつつある。このインターネット上にのみ存在する仮想銀行（サイバーバンク）においてもパスワードなどにより個人認証を行っているが、上述したような犯罪に対しては、何ら防御できず、取引契約者は不法な第三者に従わざるを得ないのが実情である。

【００１０】

【発明の目的】本発明は、かかる従来技術の有する不都合を改善し、特に、取引契約者が強盗などの犯罪に巻き込まれるなど、非常の事態に遭遇した際の自衛手段を、取引契約者に提供することができる取引システムを提供することを目的とする。

【００１１】

【課題を解決するための手段】上記目的を達成するため、請求項１に記載の発明において、取引システムは、情報の記憶手段と、取引端末装置との通信手段と、これら各手段の動作を制御する処理手段とを備える。また、前記記憶手段は、一の取引契約者ＩＤに通常暗証情報と非常時暗証情報との双方を関連付けた組合せを前記取引契約者ＩＤ毎に複数記憶するとともに、前記通常暗証情報に関連付けられた通常取引手順と、前記非常時暗証情報に関連付けられた非常時取引手順とを記憶する。そして、前記処理手段は、前記取引端末装置が認識した取引契約者ＩＤ及び暗証情報を前記通信手段を介して受信し、この取引契約者ＩＤと暗証情報との関連付けに一致する取引契約者ＩＤと通常暗証情報又は非常時暗証情報との関連付けを、前記記憶手段から検索するステップと、検索された関連付けをなす暗証情報が前記非常時暗証情報である場合、前記非常時取引手順を前記記憶手段から読み出して実行するステップと、を実行する。

【００１２】ここで、「取引契約者ＩＤ」とは、取引システムにおいて取引を行う取引契約者を特定できるＩＤをいう。取引契約者を直接的に特定するＩＤに限られず、口座番号のような取引契約に固有の識別情報などの間接的に取引契約者を特定するＩＤであってもよい。「暗証情報」とは、取引契約者を特定するための情報をいい、番号や記号または英文字から構成されるものに限られず、指紋や掌紋などの身体的特徴で構成されるものであってもよい。

【００１３】本発明によると、非常時暗証情報を受信した場合には通常取引手順ではなく非常時取引手順を実行するので、非常の事態、例えば、取引契約者が強盗などの犯罪に巻き込まれるなどの事態に遭遇した際の自衛手段を、取引契約者に提供することができる。

【００１４】また、請求項２に記載の発明では、請求項１に記載の取引システムにおいて、前記記憶手段は、一の取引契約者ＩＤについて、複数の異なる非常時暗証情報を格納すると共に、当該各非常時暗証情報について、各々異なる非常時取引手順を格納する。そして、前記処理手段は、前記検索された関連付けをなす暗証情報が前記非常時暗証情報である場合、当該非常時暗証情報に対応する非常時取引手順を前記記憶手段から選択的に読み出す。

【００１５】本発明によると、複数の非常時取引手順を取引契約者の選択事項として設定するので、非常時に遭遇した取引契約者が自らの判断で状況に応じた措置を講じることができる取引環境を提供できる。

【００１６】また、請求項３に記載の発明では、請求項１に記載の取引システムにおいて、前記記憶手段は、さらに、予め設定された非常時取引制限枠を前記取引契約者ＩＤ毎に関連付けて記憶する。そして、前記処理手段は、前記非常時取引手順として、前記受信した取引契約者ＩＤに対応する非常時取引制限枠を前記記憶手段から読み出すステップと、当該読み出した非常時取引制限枠を通常の取引可能枠に見せかけて、前記取引端末装置へ前記通信手段を介して送信するステップと、を実行する。

【００１７】本発明によると、非常時取引制限枠を取引契約者毎に設定するので、取引契約者がこうむる損害を少額に抑えることができる。

【００１８】また、請求項４に記載の発明では、請求項１に記載の取引システムにおいて、前記処理手段は、前記非常時取引手順として、前記受信した取引契約者ＩＤに基づいて非常時取引手順が要求されたことを示す報知情報を、前記通信手段を介し、当該非常時取引手順を要求した取引端末装置以外の外部装置に出力する。

【００１９】本発明によると、非常時取引手順が要求されたことを示す報知情報を出力するので、取引契約者が非常の事態に直面していることを秘密裏に発信でき、結果として取引契約者の早期救済を図ることができる。

【００２０】これらにより、前述した目的を達成しようとするものである。

【００２１】

【発明の実施の形態】〔第１実施形態〕

【００２２】以下、本発明の一実施形態を図１乃至図３に基づいて説明する。

【００２３】図１は、本発明の第１の実施形態を示すシステム全体のブロック図である。

【００２４】ネットワーク６０には、複数の取引端末装置２１～２３と、取引管理サーバ装置１０と、取引監視端末装置３０と、警察側情報センター４０やセキュリテ

ィ会社５０とがデータ通信可能に接続されている。

【００２５】ここで、警察側情報センター４０とセキュリティ会社５０とは、それぞれコンピュータシステムであり、スタンドアローンに限られずＬＡＮなどを含む一般的な情報管理システムを想定している。これら、警察側情報センター４０とセキュリティ会社５０とは、ネットワーク６０に接続された取引システムの提供者以外が管理する外部装置の例として図１に示した。

【００２６】そして、ネットワーク６０は、ＬＡＮなどを含む専用回線を用いたネットワークであってもよいし、インターネットなどの公衆回線を利用したネットワークであってもよい。なお、このネットワーク６０に接続するためのデータ回線やインターネットサービスプロバイダ（ＩＳＰ）の図示は省略している。

【００２７】また、複数の取引端末装置２１～２３、取引管理サーバ装置１０、取引監視端末装置３０、警察側情報センター４０やセキュリティ会社５０のそれぞれと、ネットワーク６０との接続は有線によるデータ通信であってもよいし、無線によるデータ通信であってもよい。

【００２８】各取引端末装置２１～２３は、取引契約者が使用する端末装置をいい、情報の入力手段２１ａ，２２ａ，２３ａ，２１ｂ，２２ｂ，２３ｂに加えて、不図示ではあるが、情報の表示手段、情報の記憶手段、外部装置との通信手段、および各手段を制御する処理手段とを備える。ただし、取引システムの業務形態に応じてその詳細な仕様は異なる。例えば、銀行やクレジットサービス会社などが取引システムを運営する場合には、本店や各支店に備えられるＡＴＭなどの現金自動預け払い機が取引端末装置となり、カード専用の無人カードサービスコーナーでは引き出し専門のＣＤなどが取引端末装置となる。

【００２９】また、入力手段２１ａ，２２ａ，２３ａ，２１ｂ，２２ｂ，２３ｂは、取引端末装置２１～２３への情報提供の態様に応じた方式のインターフェースが設けられる。例えば、ＡＴＭやＣＤでは、磁気カードを読み取るためのカードリーダーなどの第１の入力手段２１ａ，２２ａ，２３ａと暗証番号を受け付けるタッチパネルなどの第２の入力手段２１ｂ，２２ｂ，２３ｂとを備える。また、図１において入力手段の数を２つとしたが、特に限定されるものではなく、必要に応じてＩＣカードとの情報の授受を行うＩＣ用インターフェースなどの入力手段を別途備える構成としてもよいし、兼用する構成としてもよい。なお、説明の便宜上、図１には３台の取引端末装置２１～２３を示したが、ネットワークに接続される取引端末装置は特にこの数に限られるものでない。

【００３０】取引管理サーバ装置１０は、取引端末装置２１～２３を用いた取引を管理するためのサーバ装置であり、情報の記憶手段１１と、取引端末装置２１～２３との通信手段１２と、これら各手段の動作を制御する処理手段１３とを備える。なお、図１に示した取引管理サーバ装置１０は、最低限の構成を示すものであり、また、その他サーバとして必要な公知の構成および機能は、本実施形態でもそのまま備えたものとする。

【００３１】取引監視端末装置３０は、ネットワーク６０を介した取引端末装置２１～２３による取引を監視するための端末装置である。主に本発明にかかる取引システムの提供者側が取引端末装置２１～２３の稼働状況を監視することを想定している。

【００３２】ここで、図１において取引管理サーバ装置１０と取引監視端末装置３０とを各一台としているが、取引管理サーバ装置１０と取引監視端末装置３０の数は特に制約を受けるものではない。例えば、複数の取引管理サーバ装置１０により取引管理を行ってもよいし、銀行であれば本店や支店もしくはメンテナンス部門のそれぞれに取引監視端末装置３０を設けるシステム構成としてもよい。

【００３３】以上説明した各装置についてさらに詳述する。

【００３４】まず、取引管理サーバ装置１０について説明する。取引管理サーバ装置１０の記憶手段１１は、例えばＲＡＭ、ＲＯＭ、ＨＤＤ等のデータを格納することができる記憶媒体を備えるものである。ただし、特定の一の記憶媒体に限られるものではなく、複数の記憶媒体を組み合わせた構成であってもよい。

【００３５】そして、記憶手段１１は、一の取引契約者ＩＤに通常暗証情報と非常時暗証情報との双方を関連付けた組合せを取引契約者ＩＤ毎に複数記憶するとともに、通常暗証情報に関連付けられた通常取引手順と、非常時暗証情報に関連付けられた非常時取引手順とを記憶する。ここで、「暗証情報」とは、取引契約者を特定するための情報をいい、番号や記号または英文字から構成されるものに限られず、指紋や掌紋などの身体的特徴で構成されるものであってもよい。

【００３６】具体的には、図１に示したように、記憶手段１１は、通常取引手順記憶領域１１ａ、非常時取引手順記憶領域１１ｂ、および暗証情報データベース１１ｃを備える。

【００３７】ここで、通常取引手順記憶領域１１ａは、取引契約者との間で行われる真正な契約業務を実行するためのプログラム（通常取引手順）を格納する。例えば、残高照会処理手順や預金引き出し手順などが挙げられる。

【００３８】また、非常時取引手順記憶領域１１ｂは、上述した通常取引手順とは異なり、取引契約者が第三者の強要などを受け、取引契約者の意思に反して取引を行った場合への対応として、常ならざる非常の際のプログラム（非常時取引手順）を複数格納する。例えば、取引契約者が予め設定した非常時取引制限枠に応じて、非常

時の取引の際に本来の取引可能枠ではなくその非常時取引制限枠を通常の取引可能枠に見せかけて表示させる非常時取引手順や、取引契約者ＩＤに基づいて非常時取引手順が要求されたことを示す報知情報を警察当局４０やセキュリティ会社５０などの外部装置に出力する非常時取引手順などを格納する。

【００３９】ここで、「取引契約者ＩＤ」とは、取引システムにおいて取引を行う取引契約者を特定できるＩＤをいう。取引契約者を直接的に特定するＩＤに限られず、口座番号のような取引契約に固有の識別情報などの間接的に取引契約者を特定するＩＤであってもよい。また、「取引可能枠」とは、取引契約者が通常の取引において取り扱うことができる上限枠をいい、例えば、口座の預金残高や、与信に基づくキャッシングサービスの上限額などをいう。そして、「取引制限枠」とは、取引契約者が予め設定した非常時の取引における制限枠（臨界条件）をいい、例えば、実際の預金残高よりも低い一定額もしくは預金残高の５％といった一定割合や、キャッシング上限額を一定額または一定割合とするなどの条件を設定し得る。なお、制限枠は金額に限るものではなく、取引を窓口限定（ＡＴＭ等の使用不可）もしくは本店限定にするなど取引形態に対する制限を設定するものであってもよい。

【００４０】そして、暗証情報データベース１１ｃは、図２（ａ）に示すように取引契約者ＩＤに通常暗証情報と非常時暗証情報との双方を関連付けた組合せを一括して管理する。また、一の取引契約者ＩＤについて複数の異なる非常時暗証情報を格納すると共に、図２（ｂ）に示すように各非常時暗証情報と各非常時取引手順を関連付けている。これにより、上述した非常時取引手順記憶領域１１ｂとあいまって、各非常時暗証情報について、各々異なる非常時取引手順を格納する構成を実現する。

【００４１】例えば、磁気カードなどにおいて数値情報を用いる場合には、図２（ａ）に示したように、暗証情報データベース１１は、取引契約者との間の契約に基づき割り当てた口座番号０１０００１を取引契約者ＩＤとして用いる。また、その契約において、予め取引契約者が通常暗証情報として暗証番号１２３４を、前述した取引制限を行う非常時取引手順に対応した非常時暗証情報１として暗証番号４３２１と取引制限枠として５万円を設定し、警察に報知する非常時取引手順に対応した非常時暗証情報２として暗証番号５４３２を設定したときには、口座番号０１０００１とこれらの暗証番号等を関連付けて記憶する。このようにして、暗証情報データベース１１は、取引契約者ＩＤと通常暗証情報と非常時暗証情報とを一つの組合せとして、取引契約者ＩＤ毎に記憶する。

【００４２】また、ＩＣカードなどのように記憶情報量が多い場合には、例えば、通常暗証情報として右手の親指の指紋パターンを、非常時暗証情報１として左手の親指の指紋パターンを、非常時暗証情報２として左手の人差し指の指紋パターンを格納するようにしてもよい。

【００４３】なお、取引管理サーバ装置１０を複数設ける場合には、それぞれの取引管理サーバ装置１０の記憶手段１１に暗証情報データベース１１ｃ等を分散させて備える構成や、通常取引手順記憶領域１１ａを記憶し管理する取引管理サーバ装置１０と非常時取引手順記憶領域１１ｂを記憶し管理する取引管理サーバ装置１０と暗証情報データベース１１ｃを記憶し管理する取引管理サーバ装置１０とを相互接続した構成など、取引システムの設置形態に応じて選択する。

【００４４】通信手段１２は、例えばネットワークインターフェースカード（ＬＡＮボード等）やシリアルポートなどデータの授受を行うインターフェースを備えるものである。

【００４５】処理手段１３は、例えばＣＰＵ等の演算処理装置を含むものであり、記憶手段１１に対するデータの記憶（格納）処理や読み出し（取得）処理、通信手段１２に対するデータの出力処理や取得処理など、各種処理を実現する。処理に際しては、記憶手段１１の所定の領域に格納された処理手順に従う。なお、処理手順はプログラムなどのかたちで処理手段１３に対して提供される。また、これらの処理は、例えば単一のＣＰＵにより実行されるものであってもよいし、複数のＣＰＵによる分散処理がなされるものであってもよい。

【００４６】具体的には、処理手段１３は、取引端末装置２１～２３が認識した取引契約者ＩＤ及び暗証情報を通信手段１２を介して受信し、この取引契約者ＩＤと暗証情報との関連付けに一致する取引契約者ＩＤと通常暗証情報または非常時暗証情報との関連付けを、記憶手段１１の暗証情報データベース１１ｃから検索するステップと、検索された関連付けをなす暗証情報が非常時暗証情報である場合、非常時取引手順を記憶手段１１の非常時取引手順記憶領域１１ｂから読み出して実行するステップと、を実行する。

【００４７】取引端末装置２１～２３が備える、情報の入力手段２１ａ，２１ｂ，２２ａ，２２ｂ，２３ａ，２３ｂ、情報の表示手段（不図示）、情報の記憶手段（不図示）、外部装置との通信手段（不図示）、および各手段の動作を制御する情報の処理手段（不図示）は、取引契約者との間で締結した契約業務を履行する処理を行うとともに、取引端末装置２１～２３を操作する者が真正の取引契約者であるか否かを判断するための個人認証処理を行う。

【００４８】本実施形態の取引端末装置２１～２３は、個別認証の方式として、個人認証用の識別情報となる暗証情報を記憶させた磁気カードやＩＣカードから暗証情報を読み取るためのインターフェースを備え、一方で入力手段を介して取引を行う者から照合用の暗証情報の提供を受けて取引端末装置２１～２３で暗証情報のマッチ

ングをとることにより取引契約者が真正であるか否かを判別する方式を採用する。このため、本実施形態において取引契約者に対して発行されるカードには、取引契約者ＩＤと通常暗証情報と非常時暗証情報との双方が記憶されている。

【００４９】ただし、カードは、通常暗証情報と非常時暗証情報とを区別できないように記憶している。例えば、同じコード体系としたり、暗証情報が格納されるポインタをランダムなものとした上で暗号化を施すなどして、カードに記憶している。これは、カードが盗難された場合に、解読した暗証情報が通常暗証情報であるのか非常時暗証情報であるのかが判別できないようにしたものである。加えて、非常時暗証情報のバリエーションが増えるにしたがって、第三者が任意に暗証情報を選択したとしても、通常の取引を行うことができる暗証情報を引き当てる確率が低くなるため、本実施形態のようにカード自体に暗証情報を記憶させるシステムを採用する場合には、複数の非常時暗証情報を記憶させることが有効である。

【００５０】以上説明した取引システムの全体動作を図３に基づいて説明する。以下、取引端末装置２１を用いて取引契約者が取引する場合を一例としてとりあげる。図３は取引端末装置２１と取引管理サーバ装置１０のプログラム処理を示すフローチャートである。また、説明の容易のため、取引契約者の口座番号を取引契約者ＩＤとして用いるものとして説明する。

【００５１】まず、取引端末装置２１では個人認証処理を行う。具体的には、取引端末装置２１は、取引契約者から口座番号と真正の暗証情報とを受け付ける（Ｓ１）。具体的には、取引端末装置２１は、第１の入力手段２１ａ（カードから情報を読み取るカードリーダーなどの専用インターフェース）を介して、提供されたカードから口座番号と暗証情報を読み込む。ここで、カードが記憶する暗証情報は複数あるが、これらをすべて読み込む。

【００５２】さらに、第２の入力手段２１ｂ（タッチパネルや光学式スキャナなど）を介して、取引端末装置２１の利用者から照合用の暗証情報を受け付ける（Ｓ２）。そして、第１の入力手段が受け付けた真正の暗証情報と第２の入力手段が受け付けた暗証情報を比較し、一致している場合には、その利用者が真正の取引契約者であるとみなして、後述する次の処理（Ｓ４）へと移行する（Ｓ３）。ただし、照合用の暗証情報が、カードから読み出した暗証情報のいずれにも該当しない場合は、再度照合用の暗証情報を受け付ける手続へと戻り、所定の回数にわたり不一致の場合には既知のシステムと同様にそのカードは使用不可能となる。

【００５３】なお、この段階では、前述したように盗難対策の観点から、カードに格納されている暗証情報のうち、どの暗証情報が通常暗証情報で、どの暗証情報が非常時暗証情報であるかは区別できない。しかし、通常暗証情報も非常時暗証情報も取引契約者本人しか知り得ない情報として位置づけられているため、個人認証を行う上においては十分である。

【００５４】上述した取引端末装置２１における個人認証処理が完了した後は、処理の主体が取引端末装置２１から取引管理サーバ装置１０へと移る。そして、取引管理サーバ装置１０では、取引端末装置２１が受け付けた暗証情報が通常暗証情報であるのか、非常時暗証情報であるのかを判別する処理を行う。

【００５５】具体的には、まず、取引端末装置２１の処理手段は、取引端末装置２１が備える通信手段およびネットワーク６０を介して、取引管理サーバ装置１０へ、取引契約者ＩＤである口座番号と、照合した暗証情報とを送信する（Ｓ４）。

【００５６】これに対し、取引管理サーバ装置１０の処理手段１３は、取引端末装置２１が認識した取引契約者ＩＤ及び暗証情報を通信手段１２を介して受信し、記憶手段１１の所定の領域に格納する（Ｓ５）。続いて、処理手段１３は、記憶手段１１の所定の領域から取引契約者ＩＤと暗証情報を読み出し、当該読み出した取引契約者ＩＤと暗証情報との関連付けに一致する取引契約者ＩＤと通常暗証情報又は非常時暗証情報との関連付けを、記憶手段１１の暗証情報データベース１１ｃから検索する（Ｓ６）。

【００５７】そして、処理手段１３は、取引契約者ＩＤと暗証情報との組合せを照合し（Ｓ７）、検索された関連付けをなす暗証情報が非常時暗証情報である場合、非常時取引手順を記憶手段１１の非常時取引手順記憶領域１１ｂから読み出して実行する（Ｓ８～Ｓ１４）。

【００５８】ここで、非常時取引手順記憶領域１１ｂからの非常時取引手順の読み出し処理として、処理手段１３は、非常時暗証情報に対応する非常時取引手順を記憶手段１１の非常時取引手順記憶領域１１ｂから選択的に読み出す（Ｓ８，Ｓ１２）。

【００５９】具体的には、例えば、図２に示したように、検索により抽出された取引契約者ＩＤと組み合わされるのが非常時暗証情報１に分類される暗証情報である場合には、処理手段１３は、非常時暗証情報１に対応する非常時取引手順１を非常時取引手順記憶領域１１ｂから読み出し（Ｓ８）、読み出した非常時取引手順１にしたがってその非常時取引処理を実行する（Ｓ９～Ｓ１１）。

【００６０】詳細には、非常時取引手順１に従った処理は次のようになる。処理手段１３は、受信した取引契約者ＩＤに対応する非常時取引制限枠を記憶手段１１の暗証情報データベース１１ｃから読み出し、読み出した非常時取引制限枠を記憶手段１１の所定の領域に格納する（Ｓ９）。そして、格納した非常時取引制限枠を通常の取引可能枠に見せかけて、取引端末装置２１へ通信手段

１２を介して送信する（Ｓ１０）。ここで、読み出した非常時取引制限枠を通常の取引可能枠に見せかけて送信することにより、この非常時取引制限枠を受信した取引端末装置２１側においては、特別の手順を要することなく、非常時取引制限枠にしたがった取引を行うことができる（Ｓ１１）。

【００６１】一方、図２に示したように、検索により抽出された取引契約者ＩＤと組み合わされるのが非常時暗証情報２に分類される暗証情報である場合には、処理手段１３は、非常時暗証情報２に対応する非常時取引手順２を非常時取引手順記憶領域１１ｂから読み出し（Ｓ１２）、読み出した非常時取引手順２にしたがってその非常時取引処理を実行する（Ｓ１３，Ｓ１４）。

【００６２】詳細には、非常時取引手順２に従った処理は次のようになる。処理手段１３は、受信した取引契約者ＩＤに基づいて非常時取引手順が要求されたことを示す報知情報を作成し（Ｓ１３）、作成した報知情報を、通信手段１２を介し、非常時取引手順を要求した取引端末装置２１以外の外部装置に出力する（Ｓ１４）。ここで、外部装置として設定される側としては、取引監視端末装置３０や警察側情報センター４０もしくはセキュリティ会社５０などが挙げられる。いずれに報知するかは、取引システムの運用者または提供者が定めてもよいし、自衛手段のバリエーションとして、取引契約者に選択させるシステム構成としてもよい。

【００６３】処理手段１３が非常時取引手順２を実行し、取引契約者ＩＤに基づいて非常時取引手順が要求されたことを示す報知情報を出力することにより、取引契約者が非常の事態に遭遇しており、救援を必要とする旨を迅速に関係者に報知することができる。したがって、取引契約者に関わる情報を付随させた報知情報を受け取った警察等は、取引契約者が非常の取引を行っているうちに初動を開始することができ、取引契約者を早期に助けることが可能となる。

【００６４】一方、検索の結果、読み出した取引契約者ＩＤと暗証情報との関連付けに一致するのが、取引契約者ＩＤと通常暗証情報との関連付けである場合には、処理手段１３は、通常取引手順記憶領域１１ａから通常取引手順を読み出し、実行することになる（Ｓ１５）。

【００６５】以上説明したように、本実施形態の構成を採用することにより、取引契約者が非常の事態に遭遇した際の自衛手段を、取引契約者に提供できる。また、複数の非常時取引手順に応じた暗証情報を設定することができるため、取引契約者が能動的に、取引契約者がおかれた状況に応じて非常時取引手順を選択できるという、優れた自衛手段を取引契約者に提供できる取引システムを実現できる。

【００６６】なお、本実施形態は、上述した構成に限られるものではなく、非常時暗証情報と非常時取引手順とは完全な一対一の対応でなくてもよい。例えば、上述した非常時取引手順１と非常時取引手順２の双方を読み出し、実行する第３の非常時暗証情報を設定してもよい。

【００６７】また、非常時取引手順も上述したプロセスに限られるものではなく、例えば、本来強盗にあった場合に、一銭も口座に残金がないとすると余計に危険な状況に追い込まれる可能性があるので、上述したように所定の残高を表示するようにしたが、相手に応じて「回線のメンテナンス中につき他の端末を使用して下さい」と表示させたり、「回線が混み合っています。備え付けの電話にて担当者をお呼び下さい」などの表示をさせるなどの手順も採り得る。

【００６８】〔第２実施形態〕

【００６９】次に、本発明にかかる第２の実施形態を説明する。本実施形態においても、取引システムの基本的な構成は図１に示したシステムと変わりはない。また、暗証情報データベース１１ｃのデータ構造も、図２に示したデータ構造と同じである。

【００７０】ただし、本実施形態では、ゼロ認証方式を採用する取引システムや、インターネットバンキングなどの取引システムなどのように、取引端末装置２１～２３自体では個人認証を行わず、取引契約者ＩＤと暗証情報の提供を受け、受け付けた取引契約者ＩＤと暗証情報をサーバ装置に送信する処理を行い、個人認証を取引管理サーバ装置１０側で行う点で異なる。

【００７１】したがって、取引端末装置２１～２３は、具体的には、ゼロ認証方式を採用したＡＴＭやＣＤなどの場合には、第１の実施形態と同様に、口座番号などの取引契約者ＩＤを記憶したカードとのインターフェースなどの第１の入力手段と、暗証情報を受け付けるためタッチパネルなどの第２の入力手段を備える構成となる。一方、インターネットバンキングなどの取引システムにおいては、各家庭に備えられたパーソナルコンピュータやＰＤＡなどの携帯情報端末もしくは携帯電話などが取引端末装置となり、口座番号や暗証情報を受け付けるキーボードなどの入力手段が最低一つあれば足りることになる。

【００７２】以下、本実施形態にかかる取引システムの動作について、図４に基づき説明する。ここでは、図１における取引端末装置２２と取引管理サーバ装置１０との間で取引を行う場合を想定して説明する。

【００７３】まず、取引端末装置２２の処理手段は、取引契約者から取引端末装置２２が備える所定の入力手段を介して、取引契約者ＩＤと暗証情報とを受け付け、受け付けた取引契約者ＩＤと暗証情報とを取引端末装置２２が備える記憶手段の所定の領域に格納する（Ｓ２１）。本実施形態においては、取引契約者ＩＤとして、口座番号やネットバンクにおいては現金の移動の際に入力すべき口座契約者である取引契約者毎に割り振られるＩＤコードなどが該当する。

【００７４】このとき、取引端末装置２２において個人

認証を行わないので、受け付けた取引契約者ＩＤと暗証情報とを取引端末装置２２が備える通信手段およびネットワーク６０を介して取引管理サーバ装置１０へ送信する（Ｓ２２）。

【００７５】取引管理サーバ装置１０の処理手段１３は、通信手段１２を介して取引端末装置２２から送信された取引契約者ＩＤと暗証情報とを受信し、記憶手段１１の所定の領域に格納する（Ｓ２３）。

【００７６】続いて、処理手段１３は、記憶手段１１の所定の領域から受信した取引契約者ＩＤと暗証情報を読み出し、読み出した取引契約者ＩＤと暗証情報との関連付けに一致する取引契約者ＩＤと通常暗証情報又は非常時暗証情報との関連付けを、記憶手段１１の暗証情報データベース１１ｃから検索する（Ｓ２４）。

【００７７】検索の結果に基づき処理手段１３は判定を行う（Ｓ２５）。具体的には、取引契約者ＩＤと暗証情報との組合せが存在する場合には、処理手段１３は、取引契約者本人による取引であると認定し、個人認証を完了し、次の通常暗証情報か非常時暗証情報かを判定する処理へと移行する。一方、取引契約者ＩＤと暗証情報との組合せが存在しない場合には、再度、取引端末装置２２に対して、少なくとも暗証情報の再入力を求める（Ｓ２１）。

【００７８】そして、処理手段１３は、取引契約者ＩＤと暗証情報との組合せが存在する場合には、検索された関連付けをなす暗証情報が通常暗証情報であるか、またはいずれの非常時暗証情報であるかを照合する（Ｓ２６）。そして、検索された関連付けをなす暗証情報が非常時暗証情報である場合、対応する非常時取引手順を記憶手段１１の非常時取引手順記憶領域１１ｂから読み出して実行する（Ｓ２７，Ｓ２８）。

【００７９】これ以降の非常時取引手順に従う処理は、前述した第１の実施形態と同様であるので説明を省略する。

【００８０】なお、検索の結果、読み出した取引契約者ＩＤと暗証情報との関連付けに一致するのが、取引契約者ＩＤと通常暗証情報との関連付けである場合には、処理手段１３は、通常取引手順記憶領域１１ａから通常取引手順を読み出し、実行することになる（Ｓ２９）のも前述した第１の実施形態と同様である。

【００８１】本実施形態のように、取引管理サーバ装置１０側で個人認証処理を行う取引システムにおいても本発明は好適に実施でき、取引契約者が非常の事態に遭遇した際の自衛手段を、取引契約者に提供できる。また、複数の非常時取引手順に応じた暗証情報を設定することができるため、取引契約者が能動的に、取引契約者がおかれた状況に応じて非常時取引手順を選択できるという、優れた自衛手段を取引契約者に提供できる取引システムを実現できる。

【００８２】また、ネットバンキングのように監禁状態で現金引き出しを強要できる状況においても、第三者に気取られることなく取引契約者が自己の救助を訴えることができる手段を、取引システム提供者側から提供することができる。したがって、取引システム提供者側にとっても新しいサービスとしてビジネス展開におけるアドバンテージを得ることができる。

【００８３】そして、本実施形態にかかる取引システムは、上述したシステム構成に限られるものではなく、例えば、ネットバンキングにおけるクレジットサービスにおいて、取引端末装置２３と取引管理サーバ装置１０との間に、仲介販売店が介在していてもよい。具体的には、取引端末装置２３から送信される取引契約者ＩＤと暗証情報が暗号化されたままクレジットサービス会社の運営する取引管理サーバ装置１０に送信された場合に、その暗証情報が非常時取引暗証情報であり、設定した非常時取引制限枠を用いる非常時取引手順にしたがうものである場合に、仲介販売店に返信する与信に関連するネットショッピング可能額を本来の取引可能額に代えて低額の非常時取引制限枠として送信することにより、仲介販売店にさえも気付かれることなく、非常時取引手順にしたがった処理を実現できる。

【００８４】加えて、上述した第１の実施形態や第２の実施形態に示されたような取引システムが普及し、周知となれば、脅迫などによる第三者のカード不正使用の強要犯罪を未然に防ぐこともできる。なぜならば、犯罪者は、カード所有者を脅迫しても犯罪が即座に露呈し、治安当局に通報されることが予め予想されるので、脅迫行為そのものを断念すると考えられるからであり、個人認証システムの確立とともに本発明は治安向上に貢献するものであるといえる。

【００８５】

【発明の効果】本発明は、以上のように構成され機能するので、これによると、請求項１に記載の発明では、非常時暗証情報を受信した場合には通常取引手順ではなく非常時取引手順を実行するようにしたので、取引契約者が強盗などの犯罪に巻き込まれるなどの非常事態に遭遇した際の自衛手段を、取引契約者に提供することができる。

【００８６】また、請求項２に記載の発明では、複数の非常時取引手順を取引契約者の選択事項として設定するようにしたので、非常時に遭遇した取引契約者が自らの判断で状況に応じた措置を講じることができる取引環境を提供できる。

【００８７】また、請求項３に記載の発明では、非常時取引制限枠を取引契約者毎に設定するようにしたので、取引契約者がこうむる損害を少額に抑えることができる。

【００８８】また、請求項４に記載の発明では、非常時取引手順が要求されたことを示す報知情報を出力するようにしたので、取引契約者が非常の事態に直面している

15　　16

ことを秘密裏に発信でき、結果として取引契約者の早期救済を図ることができる。

【００８９】以上のように、本発明によれば、従来にない優れた取引システムを提供することができる。

【図面の簡単な説明】

【図１】本発明にかかる一実施形態の構成を示す取引システム全体のブロック図である。

【図２】図２（ａ）は、図１に示した暗証情報データベースのデータ構造の一例を示す構造図であり、図２（ｂ）は、非常時暗証情報と非常時取引手順との関連づけを定めたデータ構造の一例を示す構造図である。

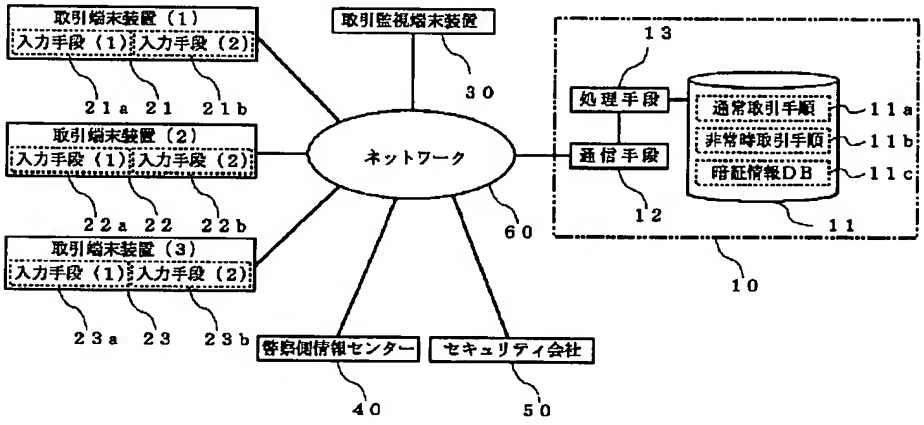
【図３】図１に示した取引システムの動作を示すフローチャートである。

【図４】本発明にかかる他の実施形態の取引システムにおける動作を示すフローチャートである。

【符号の説明】

１０　取引管理サーバ装置
１１　記憶手段
１１ａ　通常取引手順記憶領域
１１ｂ　非常時取引手順記憶領域
１１ｃ　暗証情報データベース
１２　通信手段
１３　処理手段
２１，２２，２３　取引端末装置
２１ａ，２２ａ，２３ａ　第１の入力手段
２１ｂ，２２ｂ，２３ｂ　第２の入力手段
３０　取引監視端末装置
４０　警察側情報センター
５０　セキュリティ会社
６０　ネットワーク

【図１】




【図２】

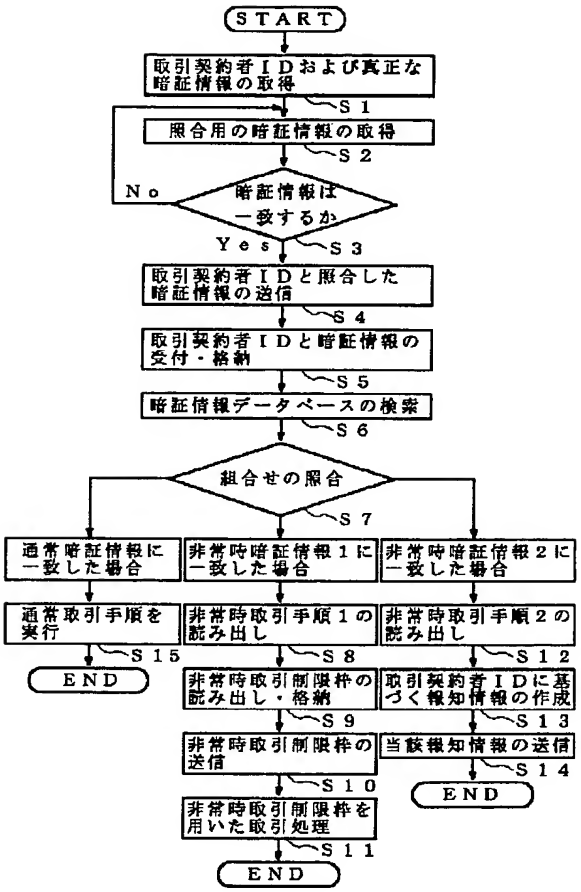
（ａ）

| 取引契約者ＩＤ | 通常暗証情報 | 非常時暗証情報１ | 設定取引制限枠 | 非常時暗証情報２ |
|---|---|---|---|---|
| ０１０００１ | １２３４ | ４３２１ | ５００００ | ５４３２ |
| ・ | ・ | ・ | ・ | ・ |
| ・ | ・ | ・ | ・ | ・ |
| ・ | ・ | ・ | ・ | ・ |

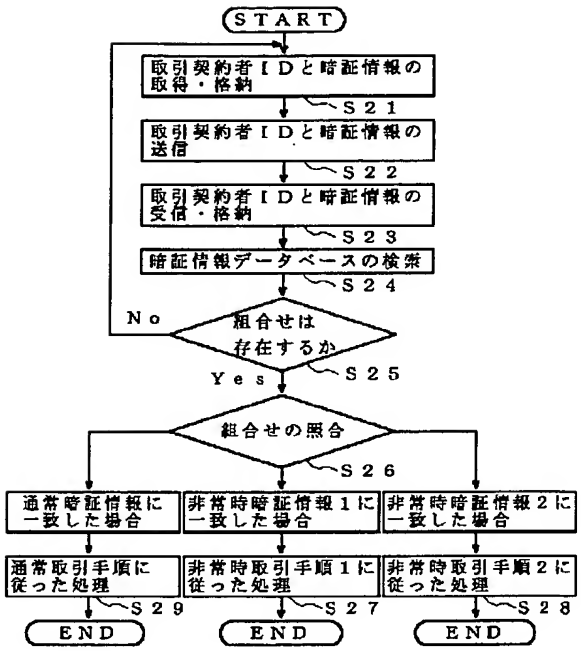
（ｂ）

| 非常時暗証情報 | 非常時取引手順 |
|---|---|
| 非常時暗証情報１ | 非常時取引手順１ |
| 非常時暗証情報２ | 非常時取引手順２ |
| ・ | ・ |
| ・ | ・ |

【図３】


START
取引契約者ＩＤおよび真正な暗証情報の取得
Ｓ１
照合用の暗証情報の取得
Ｓ２
No
暗証情報は一致するか
Yes
Ｓ３
取引契約者ＩＤと照合した暗証情報の送信
Ｓ４
取引契約者ＩＤと暗証情報の受付・格納
Ｓ５
暗証情報データベースの検索
Ｓ６
組合せの照合
Ｓ７
通常暗証情報に一致した場合
非常時暗証情報１に一致した場合
非常時暗証情報２に一致した場合
通常取引手順を実行
非常時取引手順１の読み出し
非常時取引手順２の読み出し
Ｓ１５
Ｓ８
Ｓ１２
END
非常時取引制限枠の読み出し・格納
取引契約者ＩＤに基づく報知情報の作成
Ｓ９
Ｓ１３
非常時取引制限枠の送信
当該報知情報の送信
Ｓ１０
Ｓ１４
END
非常時取引制限枠を用いた取引処理
Ｓ１１
END

【図４】


START
取引契約者ＩＤと暗証情報の取得・格納
Ｓ２１
取引契約者ＩＤと暗証情報の送信
Ｓ２２
取引契約者ＩＤと暗証情報の受信・格納
Ｓ２３
暗証情報データベースの検索
Ｓ２４
No
組合せは存在するか
Yes
Ｓ２５
組合せの照合
Ｓ２６
通常暗証情報に一致した場合
非常時暗証情報１に一致した場合
非常時暗証情報２に一致した場合
通常取引手順に従った処理
非常時取引手順１に従った処理
非常時取引手順２に従った処理
Ｓ２９
Ｓ２７
Ｓ２８
END
END
END